REMARKS

In the ***final*** Office Action mailed November 5, 2009 the Office noted that claims 1-9, 11-21, 23-30, 32, 33, 35-40 were pending and rejected claims 1-9, 11-21, 23-30, 32, 33, 35-40. Claims 1, 17 and 26 have been amended, no claims have been canceled, and, thus, in view of the foregoing claims 1-9, 11-21, 23-30, 32, 33, 35-40 remain pending for reconsideration which is requested. No new matter has been added. The Office's rejections are traversed below.

CLAIM OBJECTION

Claim 17 stands objected to for informalities. In particular, the Office asserts that the claim contains a typographical error. The Applicants have amended the claims to overcome the rejection.

Withdrawal of the rejection is respectfully requested.

REJECTIONS under 35 U.S.C. § 102

Claims 1-4, 8, 9, 11-21, 23-28, 32, 33 and 35-40 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Naccache, U.S. Patent No. 7,168,065. The Applicants respectfully disagree and traverse the rejection with an argument and amendment.

Naccache discusses a system wherein the execution of a set of instructions is made secure by computing a signature during the execution of these instructions and by comparing the obtained signature with a predetermined signature. To that end, the set of instructions comprises a first instruction for initializing the calculation of the signature and a last instruction for comparing the obtained signature with the predetermined signature. The way according to which the signature is calculated is predetermined. In other words, the microcontroller that executes the set of instructions comprises a dedicated function for computing a signature according to an initialization value and the executed instructions.

Claim 1 has been amended to recite "wherein said set of instructions comprises at least one ***first*** instruction for initializing the calculation of the second signature, at least one ***second*** instruction for controlling the calculation ***mode*** of the second signature, ***and a third instruction, different than the at least one second instruction, for comparing the second signature obtained according to the at least one second***

instruction with the first signature." (Emphasis added) Support for the amendment may be found, for example, in the annex where the instructions A 1, B3, C3, and D1 correspond to instructions for initializing the calculation of the signature, instructions A2 and A12, B7, C7 and C8, and D11 correspond to instructions for controlling the calculation of the signature, and instructions A13, B8, C9 and C10, and D12 correspond to instructions for comparing the obtained signature with a predetermined signature. The Applicants submit that no new matter is believed to have been added by the amendment of claim 1. Claims 17 and 26 have been amended in a manner consistent with the amendment to claim 1.

In Naccache, the program for which execution is monitored comprises functional instructions Inst.1 to Inst.n and two additional monitoring instructions Inst.0 and Inst.n+1 (Naccache, col. 9, lines 18-20 and col. 10, lines 30-32). The first monitoring instruction initializes a hash value (VH), that is to say a signature (Naccache, col. 9, lines 27-28). It is placed before the first functional instruction Inst.1. The second monitoring instruction is related to the comparison between the calculated hash value (VHn) and a reference value (Vref) specified in this instruction (Naccache, col. 9, lines 61-64). It is placed following the last functional instruction Inst.n.

The hash value is calculated according to a predetermined recursive scheme. For a functional instruction

Inst.i+1 of the program that execution is monitored, the hash value (VHi+1) is calculated as a function of the hash value (VHi) calculated for the previous functional instruction Inst.i and of the value of the instruction Inst.i+1. As a consequence, the hash value VHn depends on its initialization value and on the functional instructions Inst.1 to Inst.n but does not depend on monitoring instruction Inst.n+1.

Thus, when the Office asserts that the second monitoring instruction finalizes the hash function and that, consequently, the second monitoring instruction is an instruction for controlling the calculation of the hash value, the Office assimilates the control of the execution of the calculation of a value with the control of the calculation of such a value, which is incorrect. This is confirmed by the two embodiments disclosed by reference to Figs. 3 and 4 according to which the calculated hash values are equals while being calculated before and after reaching the second monitoring instruction. In other words, the second monitoring instruction has no effect on the calculated hash value.

As a consequence, finalizing the hashing function should not be considered as equivalent to controlling the calculation of a value according to which the calculated value depends on the controlling instructions.

As Naccache teaches a system wherein the execution of a set of instructions is made secure by computing a signature

during the execution of these instructions and by comparing the obtained signature with a predetermined signature, the set of instructions comprises a first monitoring instruction for initializing the calculation of the signature and a second monitoring instruction for comparing the obtained signature with a predetermined signature. The way according to which the signature is calculated is predetermined and is independent of the second monitoring instruction as discussed above. In other words, the microcontroller that executes the set of instructions comprises a dedicated function for computing a signature according to an initialization value and the executed instructions that is independent of the second monitoring instruction.

This is different than the claimed invention wherein the way the signature is calculated is determined according to instructions of the set of instructions. To that end, the set of instructions comprises at least one instruction for initializing the calculation of the signature (e.g. A1, B3, C3, and D1 of the examples given in Annex), at least one instruction for controlling the calculation of the second signature (e.g. A2 and A12, B7, C7 and C8, and D11), and at least one instruction for comparing the obtained signature with a predetermined signature (e.g. A13, B8, C9 and C10, and D12).

Therefore, Naccache does not disclose the use of three distinct monitoring instructions for initializing the calculation

of a signature, controlling the calculation of the signature, and comparing the calculated signature with another.

It is noted that even if it is considered that the program that execution is monitored comprises several sets of instructions, each set of instructions starting with a first monitoring instruction and ending with a second monitoring instruction, Naccache does not anticipate the invention as claimed. Indeed, by considering a first second monitoring instruction belonging to a first set of instructions that would be assimilated to the claimed instruction for controlling the calculation of the second signature in the sense given by the Office and a second second monitoring instruction belonging to a second set of instructions that would be assimilated to the claimed instruction for comparing signatures, such second second monitoring instruction would not compare a signature obtained according to first second monitoring instruction with another. Therefore, even under such an interpretation, the claimed invention is not disclosed by Naccache.

Further, since the way the signature is calculated is predetermined in Naccache, the one of ordinary skilled in the art was not prompted to modify the teaching of Naccache to add instructions for controlling the calculation of the signature.

Further, since such instructions would have been useless, the one of ordinary skilled in the art would not have included them in the set of instructions. As a consequence, the

claimed invention should be considered as inventive over Naccache.

Further, since the way the signature is calculated is predetermined in Naccache, then one of ordinary skill in the art would not modify the teaching of Naccache to add instructions for controlling the calculation of the signature. And, since such instructions would have been useless, one of ordinary skill in the art would not have included them in the set of instructions. As a consequence, the claimed invention should be considered as inventive over Naccache.

For at least the reasons discussed above, claims 1, 17 and 26, and the claims dependent therefrom are not anticipated by Naccache.

Withdrawal of the rejection is respectfully requested.

REJECTIONS under 35 U.S.C. § 103

Claims 5-7, 29 and 30 stand rejected under 35 U.S.C. § 103(a) as being obvious over Naccache. The Applicants respectfully disagree and traverse the rejection with an argument.

The arguments made above to the rejection of the claims for anticipation apply likewise to the rejection for obviousness here.

For at least the reasons discussed above, Naccache fails to render obvious claims 5-7, 29 and 30.

Withdrawal of the rejection is respectfully requested.

SUMMARY

It is submitted that the claims satisfy the requirements of 35 U.S.C. §§ 102 and 103. It is also submitted that claims 1-9, 11-21, 23-30, 32, 33, 35-40 continue to be allowable. It is further submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/James J. Livingston, Jr./

James J. Livingston, Jr.
Reg.No. 55,394
209 Madison St, Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JJL/jr